Pradeep **Kumar**

Research Statement

My research interest is to have a detailed study of security issues in an unanticipated software design environment, particularly trustless computing using distributed knowledge sharing between components. This research could be applied to Automated Car, Agent-based Transformers, Application security, and distributed data migration. By designing the software system with pre-build knowledge about the unanticipated software behaviour evolution, we facilitate the developer and software Architect to mitigate the security threats at the software design stage itself.

Evidence of Excellence in Applied Encryption and Security

- **Research on Applied Encryption:** Designed the first, novel dynamic key generation and key authentication for Android Application, called Mutent –
  - **Trustless Communication Model:** Sender and Receiver can exchange sensitive, private data without prior knowledge about the participating context.
  - **Future Plans for Mutent:** Currently Mutent uses symmetric key, however I plan to modify it using Quantum Key distribution model.
- **Research on Homomorphic Encryption:** From 2019, I am working on a novel S-Box model and homomorphic encryption methodology, which theoretically evaluated and found that it takes 1 Googol year to decrypt the data.

I am interested in Security and Software modelling, particularly in the Design and Analysis of Context-Aware securities (a key behind Edge/Fog computing, Health-care data sharing, and Automated Learning system), Automation of Behaviour Analysis models based on Knowledge Graphs, and Distributed Security Mitigation using dynamic knowledge sharing. I am highly interested to continue my efforts in Designing Secure, Continuous Learning Systems research and understanding the conceptual connections between complex dynamic evolving systems and complex intelligent systems.

Evidence of Excellence in Programming Language Research

During my days as research graduate in Anna University, I have been exposed to the various facets of Computer Science excellent facilities, courses and faculty giving me a firm background of the research fundamentals and focus in Computer Science.

I find great focus and passion for research when my first research paper entitled “Modal Logics and Ownership Types – Uniting three worlds” got accepted in OOPSLA’06 Doctoral Symposium. I was 23 when I started working on modal logic and proposed the idea of merging Modal Logics and Ownership types: a novel method to dynamically control the objects’ behavior. Being a Masters’ student, I got a special permission from the OOPSLA committee to present my work in the Doctoral symposium where only Ph.D. students can participate and got $1000 travel grant. As per my knowledge, this is the first study to merge modal logics and ownership types. This work sowed seeds to all my other research in Programming Language and Security.

In 2007 (with inspiration from Sophia Drossopollou's paper on Imperative Object-based Calculus), I have designed an object calculus (named: "dot calculus") that represents delegation, ownership types and dynamic permission-based access control. Followed by **dotCalculus**, I have designed and implemented an executable language namely **dotJava**. The dotJava is the first language model to combine pass-by-value delegation and ownership types. In the presence of pass-by-value delegation, the language design gives me two major challenges like (1) multi-methods and (2) contravariant methods, which I handled using Matching types and method indexing. My graduate thesis was on ownership transfer in a class-based language based on the above two works 'dotJava' and 'dotCalculus'.

In 2008, I started my working on dependent types and proposed a novel mechanism to design a flexible aliasing mechanism using alias count. Extention to this work is **Typelets** - the first research work to combine the Dependent Types with JML - a mechanism to express the dynamic access control, singleton pattern, threads etc. using numbers. I presented this in SPLASH 2010 Poster and got appreciation and comments from by Prof.Gary T. Leavens. During this conference, I got an opportunity to discuss my language for blind people **JBrille** to Jon L. White (General Chair ILC'2010). He appreciated the project and gave suggestion on how to improve the language by using intelligent composition and also suggested me to stay with blind people for few months to understand their life (Though I was unable, to stay due to my job, I made frequent visit to blind schools to understand their way of thinking).

One of my very interesting work in the field of language-based information flow security, and type system is the **Trusted Ownership**, a novel method to dynamically controlling the access of the declassified information using trusted ownership types and access control policy. I presented the work at IWACO'2014 workshop co-located with ECOOP'14 and got good appreciation from the Programming Language Aliasing community (esp. from Prof. Sophia Drossopoulou). The implementation of trusted ownership is available in (https://github.com/trustedownership/jtrust).

I am interested in Programming Language Security and Software modeling, particularly in the Design and Analysis of Language-based securities and ownership type system. My passion for programming language design made me work on the language research during my late nights and on my free weekends in parallel to my regular chores. I am highly interested to continue my efforts in programming language and type system and logics research and to understand the conceptual connections between complex dynamic evolving systems and complex intelligent systems. Presently, I am working on a language model that combines ownership types and proof-carrying-code novel mechanism that will help in establishing trust at the object level.

Blockchain, AI/ML, & Android Security

Some of my noteworthy research innovations include:

1. **Requirement Analysis:** A novel Blockchain Metrics combining Software Automation, NLP, and Blockchain Environment, called "Blockchain Digitizability Metrics" (a method to identify the digitizability from requirements).
2. **Blockchain for E-Governance and Supply Chain Security:** Presented a novel Key-Generation technique at Block Chain Innovation Challenge, Tempe, AZ. Also presented a novel technique to solve Shadow Attacks in E-Government Document Sharing.
3. **Android Component-Level IPC Encryption:** A combination of Symmetric Key Encryption technique and "Trustless-Computing Base (TCB)", protecting apps from unknown IPC attacks.
4. **Arc Policy Language:** Designed a lightweight policy language used in Android IPC to securely communicate between apps.
5. **Privilege Leaks:** Addressing one of the upcoming key security issues that can lead to "*Leaky NFC Privileges"* and *"Shadow Attacks"*

6. **Mahalanobis Distance-Based Malware Detection Tool:** A technique that combines Binary Analysis and Machine Learning model with Mahalanobis distance metrics (rather than using Euclidean) to identify the vulnerable app without installation.

Career Goal: A good research career can only be built above the firm foundation of a good education and knowledge sharing. I am confident that I would be able to make a positive contribution to ongoing research work on your Team. Having decided that I will engage in the pursuit of a career in research and teaching, I am fully aware of the implications. I am aware of the kind of dedication, resilience and resolve that it calls for. I feel that I am adequately prepared, both in having the technical qualifications and in having the right mindset for doctoral-level research work. My long-term goal is to be a professor and researcher in computer science and pursue a career in teaching and research.